L'e-pv ou le procès-verbal électronique de constatation d'infractions en droit pénal social

Losdyck, Bénédicte; Vanreck, Odile

Published in:
Vie privée et données à caractère personnel

Publication date:
2015

Document Version
le PDF de l'éditeur

CHAPITRE 12.1. L'E-PV OU LE PROCÈS-VERBAL ÉLECTRONIQUE DE CONSTATATION D'INFRACTIONS EN DROIT PÉNAL SOCIAL

Bénédicte LOSDYCKBénédicte LOSDYCK et Odile VANRECK[1]

1. Introduction

Dans une société où tous les aspects de la vie quotidienne sont influencés par l'utilisation des techniques de l'information et de la communication, où tant les échanges commerciaux que les relations personnelles ont lieu en ligne, le bon fonctionnement de l'État passe, lui aussi, par la mise en œuvre d'un gouvernement électronique ou « e-gouvernement ».

L'e-gouvernement est un terme générique recouvrant « l'ensemble des utilisations des technologies de l'information et de la communication dans l'administration, ainsi que les mutations que ces utilisations engendrent au sein de cette matière »[2].

Dans les administrations, de nouveaux outils technologiques sont mis en œuvre à la fois pour faciliter les démarches administratives pour les citoyens et pour « renforcer l'efficacité de l'administration »[3]. Ainsi, dans le cadre de ce second objectif, on peut notamment pointer l'existence de systèmes, comme tel qu'OASIS[4] qui consiste en un entrepôt de données contenant une quantité très importante d'informations relatives aux travailleurs et employeurs, et permettant « aux différents services d'inspection sociale de combattre la fraude de manière systématique et structurée en

1. Odile Vanreck et Bénédicte Losdyck sont chercheuses au CRIDS et travaillent sur le projet de recherche HECTOR (Hybrid Electronic Curation and Transformation of Records) financé par BELSPO : BRAIN-be (Belgian Research Action through Interdisciplinary Networks).
2. E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Collection du CRIDS, Bruxelles, Larcier, 2014, p. 19.
3. *Ibid*., p. 35.
4. Ou « Organisation Anti-fraude des Services d'Inspection Sociale ».

détectant les cas potentiellement frauduleux »[1], par un profilage détaillé des personnes concernées[2].

Parmi les initiatives prises en matière d'e-gouvernement, le présent article s'attache à faire le point sur le procès-verbal électronique de constatation d'infractions existant depuis peu en droit pénal social (ci-après, « e-PV »). Ce nouveau système d'e-PV a été récemment créé et mis en œuvre afin de lutter de manière plus efficace contre le travail illégal et la fraude sociale.

Nous nous proposons d'analyser les articles du Code pénal social (en abrégé, C. pén. soc.) spécifiques au système e-PV, dispositions qui fixent le cadre légal relatif à la création et à l'utilisation de ces procès-verbaux électroniques. Après avoir décrit le système mis en place en matière d'échange électronique d'informations entre les acteurs de la lutte contre le travail illégal et la fraude sociale, nous nous attacherons au sort réservé aux données à caractère personnel figurant dans ces e-PV. Ensuite, nous examinerons si un tel document numérique a vocation à remplacer son homologue papier. Enfin, nous verrons dans quel processus plus global de gestion des documents s'inscrit ce procès-verbal électronique.

1.1. Code pénal social et ses dispositions spécifiques à l'e-PV

Toutes les dispositions pénales en droit social ont été codifiées au sein du Code pénal social. Ce nouveau Code reprend, dans un souci de simplification et de clarification, l'entièreté des dispositions pénales relatives au droit du travail et à la sécurité sociale.

Depuis son entrée en vigueur le 1er juillet 2011[3], il est désormais plus facile, tant pour l'employeur que pour le travailleur, de prendre connaissance de l'ensemble des infractions et des sanctions susceptibles d'être encourues en droit pénal social. Cette codification s'articule autour de différentes thématiques, telles que les obligations des travailleurs, des employeurs et des assurés sociaux ainsi que les modalités des poursuites de l'inspection sociale.

Moins d'un an après l'entrée en vigueur du Code pénal social, un chapitre 5 portant sur la réglementation de certains aspects de l'échange électronique d'informations entre les acteurs de la lutte contre le travail illégal et la fraude sociale y fut inséré par la loi-programme du 29 mars 2012[4]. Ces nouvelles dispositions légales fournissent

1. Banque-carrefour de la sécurité sociale, « La banque Carrefour de la Sécurité Sociale comme moteur de l'e-government du secteur social », www.ksz-bcss.fgov.be, 2014, p. 19.
2. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Collection du CRIDS, Larcier, Bruxelles, 2014, pp. 74-75.
3. Loi du 2 juin 2010 comportant des dispositions de droit pénal social, *M.B.*, 1er juillet 2010, et loi du 6 juin 2010 introduisant le Code pénal social, *M.B.*, 1er juillet 2010.
4. Loi-programme du 29 mars 2012, *M.B.*, 6 avril 2012.

un cadre général pour le procès-verbal électronique en droit pénal social. En vue de l'échange électronique d'informations entre les acteurs de la lutte contre le travail illégal et la fraude sociale, les inspecteurs sociaux établissent leurs procès-verbaux constatant des infractions de façon électronique via une application informatique conçue à cet effet[1].

L'insertion de ce chapitre a entraîné la création de l'e-PV et fournit un cadre légal prescrivant le fonctionnement de la banque de données e-PV et de la banque de données GINAA[2,3]. De plus, l'échange électronique d'informations entre les acteurs, tel qu'il est désormais prévu, se fait conformément aux dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée[4] et à la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale[5].

De manière plus précise, les nouveaux articles 100/1 à 100/13 du Code pénal social encadrent la création et l'organisation :

- d'un procès-verbal électronique uniforme, défini comme étant « le procès-verbal de constatation d'infractions établi, enregistré et envoyé au moyen de l'application informatique conçue à cette fin conformément au modèle visé à l'article 100/2 »[6] ;
- de la banque de données e-PV qui contient toutes les données reprises dans l'e-PV ainsi que ses annexes ;
- de la banque de données GINAA ;
- de flux de données résultant de l'e-PV, c'est-à-dire l'échange d'informations entre les acteurs impliqués par le biais d'un accès à la banque de données e-PV[7].

1. C.P.V.P., Rapport annuel 2012, http://www.privacycommission.be, 2012,
2. GINAA est l'acronyme de « Geïntegreerde Informatica-applicaties Administratieve », ce qui signifie en français « Applications informatiques intégrées en matière d'amendes administratives ». Il s'agit de la banque de données interne à la Direction des amendes administratives.
3. Article 100/1 C. pén. soc.
4. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
5. Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990.
6. Article 16, 7°, C. pén. soc.
7. Voy. article 100/10 C. pén. soc. et aussi C.P.V.P., avis n° 05/2012 du 8 février 2012, pp. 2 et 3.

En vertu de l'arrêté royal du 10 juillet 2013, les inspecteurs sociaux des services d'inspection sociale suivants sont habilités à établir leurs procès-verbaux de constatation d'infractions de manière électronique :

- la Direction générale Contrôle des lois sociales du Service public fédéral Emploi, Travail et Concertation sociale (ci-après, « SPF ETCS ») depuis le 10 août 2013 ;
- l'Inspection sociale du Service public fédéral Sécurité sociale (ci-après, « SPF SS ») depuis le 10 août 2013 ;
- le service d'inspection de l'Office national de l'emploi (ci-après, « ONEM ») depuis le 10 août 2013 ;
- la Direction générale des services d'inspection de l'Office national de Sécurité sociale (ci-après, « ONSS ») depuis le 10 août 2013 ;
- la Direction générale Contrôle du bien-être au travail du Service public fédéral Emploi, Travail et Concertation sociale depuis le 1er janvier 2014 ;
- le service du contrôle administratif de l'Institut national d'assurance maladie-invalidité (ci-après, « INAMI ») depuis le 31 décembre 2014 ;
- l'Inspection de l'Institut national d'assurances sociales pour travailleurs indépendants (ci-après, « INASTI ») depuis le 31 décembre 2014[1]
- l'inspection sociale de la Région wallonne depuis le 1er janvier 2015.
- l'inspection sociale de la Région de Bruxelles-Capitale depuis le 1er mars 2015.

Le gouvernement a souhaité, en insérant ces dispositions au sein du Code pénal social, intensifier la lutte contre la fraude sociale. En centralisant les procès-verbaux dans une banque de données unique et en automatisant le transfert de ces données, les services d'inspection peuvent partager plus aisément et plus rapidement entre eux des informations nécessaires dans le cadre de leur mission.

1.2. Développement du système e-PV

Pour parvenir au système tel que prévu actuellement dans le Code pénal social et développé ci-après, un long travail de réflexion, de concertation et d'analyse a été réalisé. La préparation des nouveaux articles du Code pénal social relatifs au système e-PV a duré plus de deux ans[2].

Le système e-PV s'est mis en place progressivement et a fait l'objet de mises à jour régulières.

1. Arrêté royal du 10 juillet 2013 portant exécution du chapitre 5 « Réglementation de certains aspects de l'échange électronique d'information entre les acteurs de la lutte contre le travail illégal et la fraude sociale » du titre 5 du Livre Ier du Code pénal social, *M.B.*, 31 juillet 2013.
2. Projet de loi-programme, *Doc. parl.*, Sénat, 2011-2012, n° 1545/5, p. 4.

Depuis le 3 avril 2006, la banque de données GINAA reprenant les applications informatiques des amendes administratives est fonctionnelle[1].

Dès 2009, il a été procédé à l'analyse du choix du matériel et du logiciel en partant d'un cas d'étude spécifique, celui du SPF ETCS[2]. L'année 2010 a été consacrée au développement d'une banque de données et d'un modèle d'e-PV uniforme.

En janvier 2011, l'e-PV a d'abord fait l'objet d'une phase d'essai auprès d'une vingtaine d'inspecteurs, avant d'être réellement introduit sur le terrain et de devenir opérationnel dans les quatre grands services d'inspection sociale que sont l'Inspection sociale (SPF SS), le Contrôle des lois sociales (SPF ETCS), l'inspection de l'O.N.S.S. et l'inspection de l'ONEM[3].

Ces services d'inspection disposent, depuis le mois de mars 2011, « d'un flux de travail électronique commun pour leurs PV »[4]. Notons pour information qu'en 2011, ces quatre services d'inspection dressaient annuellement 87 % des procès-verbaux établis pour les infractions du travail[5] et le millier d'inspecteurs qui les composent a reçu une formation sur le système e-PV.

En décembre 2011, la fédération de l'industrie technologique Agoria a décerné un *e-Government Award* au projet e-PV, qui, parmi les projets ICT de l'État, a été élu le plus rentable.

Dès 2012, la deuxième phase du projet a débuté et a consisté dans la correction des bugs et l'amélioration du système.

Par ailleurs, de nouveaux partenaires ont récemment pris part au projet. Il s'agit de l'INAMI, de l'INASTI[6] et des services d'inspection sociale de la Région de Bruxelles-Capitale et de la Wallonie[7]. L'arrivée de nouveaux participants tels que l'inspection Emploi et Économie sociale de la Communauté flamande et la Direction générale de l'inspection économique devrait avoir lieu dans les années à venir[8]. Au plus le nombre de services d'inspection participant sera grand, au plus les bénéfices du projet seront importants.

1. Justification du budget général des dépenses pour l'année budgétaire 2015, *Doc. parl.*, Chambre, 2014-2015, n° 0497/015, p. 15.
2. Questions et réponses écrites, *Doc. parl.*, Chambre, 2012-2013, n° 53/099, p. 143.
3. Communiqué de presse de Carl Devlies, Secrétaire d'État à la Coordination de la lutte contre la fraude, 5 janvier 2011, p. 1.
4. SMALS, Rapport d'activités 2010, https://www.smals.be, p. 25.
5. Communiqué de presse de Carl Devlies, Secrétaire d'État à la Coordination de la lutte contre la fraude, 5 janvier 2011, p. 1.
6. Arrêté royal du 10 juillet 2013 portant exécution du chapitre 5 « Réglementation de certains aspects de l'échange électronique d'information entre les acteurs de la lutte contre le travail illégal et la fraude sociale » du titre 5 du Livre 1er du Code pénal social, *M.B.*, 31 juillet 2013.
7. Projet de loi-programme, *Doc. parl.*, Sénat, 2011-2012, n° 1545/5, p. 9.
8. *Ibid*.

Actuellement, des discussions portent, d'une part, sur la manière dont le SPF Justice pourra intégrer les notifications de renonciation aux poursuites pénales dans la banque de données GINAA[1] et, d'autre part, sur les adaptations nécessaires dont l'application e-PV doit faire l'objet pour permettre l'adhésion de nouveaux partenaires[2].

1.3. Avantages de l'e-PV

Dans la lutte contre la fraude sociale, l'e-PV présente de nombreux avantages.

Tout d'abord, et cela est profitable à l'entièreté des acteurs concernés, les procès-verbaux sont de meilleure qualité. Ils sont plus complets, plus structurés et, par conséquent, plus lisibles. En effet, le modèle structuré uniforme permet que les mêmes données se retrouvent toujours au même endroit. Le système mis en place permet également un traitement plus rapide des procès-verbaux[3].

Le verbalisant bénéficie directement de cette manière uniforme de dresser des procès-verbaux et son travail est simplifié grâce à divers outils tels que la mise en place d'une application Web conviviale, un soutien à la mise en page (menus déroulants, zones à compléter préalablement définies, remplissage de certaines données automatiquement, etc.), des outils d'aide à la rédaction, des formations à l'utilisation de l'application ou un système de numérotation uniforme des procès-verbaux. Cette numérotation uniforme offre la possibilité de suivre un procès-verbal du début à la fin. En outre ont été mises en place des règles uniformes pour la consultation des procès-verbaux. De manière générale, le travail du verbalisant semble être facilité[4].

Ensuite, les divers services d'inspection utilisant les e-PV profitent tout autant de ces avantages, principalement par l'aboutissement à de meilleurs résultats. Ainsi, la meilleure qualité des procès-verbaux engendre des probabilités plus élevées de donner des suites au dossier. La faculté d'avoir accès aux informations sous format électronique et l'enregistrement dans des banques de données permettent, quant à eux, non seulement un traitement plus rapide des données, mais également la réalisation de statistiques. Par ailleurs, l'échange des informations est facilité[5] et la liaison avec des sources authentiques telles que le Registre national et une liste prédéfinie d'infractions permettent d'éviter des erreurs de forme[6].

1. Justification du budget général des dépenses pour l'année budgétaire 2015, *op. cit.,* p. 15.
2. Questions et réponses écrites, *Doc. parl*., Chambre, 2012-2013, n° 53/099, p. 144.
3. *Manuel e-PV*, version du 20 mai 2014, https://www.socialsecurity.be, pp. 3 et 4.
4. *Manuel e-PV*, *op. cit.*, pp. 3 et 4 ; M. Morsa, *Les inspections sociales en mouvement*, Bruxelles, Larcier, 2010, pp. 174 et 175 ; TP 24 février, 2081/001, pp. 55 et 56.
5. *Manuel e-PV*, *op. cit*., pp. 3 et 4.
6. SMALS, Rapport d'activités 2010, *op.cit*., p.25.

De plus, l'e-PV présente aussi des intérêts pour ses destinataires que sont, d'une part, la Justice et la Direction des amendes administratives (ci-après DAA) et, d'autre part, le contrevenant. Les droits de la défense de ce dernier sont mieux protégés grâce à la meilleure lisibilité du procès-verbal et à sa qualité, et au traitement plus rapide de son dossier[1]. La lisibilité et la qualité du procès-verbal, mais également l'encodage unique des données, sont également appréciés pour les acteurs au sein de la Justice (p. ex., le procureur du Roi ou le juge d'instruction qui reçoit le procès-verbal) et de la Direction des amendes administratives, puisque cela facilite le traitement des dossiers[2]. Par ailleurs les procès-verbaux définitifs sont envoyés de manière automatique à la Direction des amendes administratives, ce qui facilite également le travail de cette entité[3].

Enfin, des avantages économiques sont également à prendre en considération, puisque la SMALS, qui gère la partie technique de cette application et héberge la banque de données e-PV, prédisait, dans son rapport d'activités de 2010, que « la meilleure qualité des dossiers permettra à l'État belge d'encaisser chaque année jusqu'à 5,1 millions d'euros de bénéfices »[4]. De son côté, le secrétaire d'État à la Coordination de la lutte contre la fraude sociale de l'époque, Carl Devlies, indiquait que « 4 millions d'euros d'amendes administratives étaient infligés par an, mais que seuls trois quarts de ce montant étaient effectivement perçus »[5]. L'objectif de l'instauration de l'e-PV est dès lors de percevoir la totalité de cette somme.

2. Présentation du système e-PV

Avant d'aborder les défis juridiques posés par le système e-PV, il convient de le présenter en commençant, d'une part, par décrire les divers outils informatiques qui ont été créés pour mettre en place ce système et, d'autre part, par expliciter deux mécanismes propres aux e-PV, à savoir le processus de rédaction et les règles en matière d'accès.

1. Justification du budget général des dépenses pour l'année budgétaire 2015, *op. cit.*, p. 31.
2. M. Morsa, *op. cit.*, p. 174 ; *Manuel e-PV*, *op. cit.*, p. 4.
3. *Manuel e-PV*, *op. cit.*, p. 57.
4. SMALS, Rapport d'activités 2010, *op. cit.*, p. 25.
5. http://www.peoplesphere.be/fr/art/3033/un-pv-electronique-pour-tous-les-services-dinspection-sociale.

2.1. Description des outils informatiques impliqués dans le système e-PV

Les différents outils informatiques impliqués dans le système e-PV méritent que l'on s'attarde à leur définition.

2.1.1. Application e-PV

L'application e-PV est l'application informatique employée par les inspecteurs sociaux afin de dresser des procès-verbaux portant constatation d'infractions, conformément au modèle uniforme déterminé par le Comité de gestion de la banque de données e-PV[1]. L'application se trouve sur le portail de la Sécurité sociale et n'est accessible que via l'Extranet des institutions concernées[2]. Seuls les inspecteurs sociaux peuvent se connecter à cette application, et ce, par le biais de leur carte d'identité électronique[3].

Des informations relatives au Comité de gestion de la banque e-PV, comme sa composition ou ses compétences, sont fournies à l'article 100/8 du Code pénal social. Parmi ses compétences, nous pouvons pointer la gestion de la banque de données e-PV ou la prise d'initiatives afin d'améliorer l'efficacité du fonctionnement de cette banque de données.

En sus de l'application e-PV, deux banques de données ont également été conçues : la banque de données e-PV et la banque de données GINAA.

2.1.2. Banque de données e-PV

La banque de données e-PV, définie à l'article 16, 18°, du Code pénal social comme étant « la banque de données […] dans laquelle sont intégrées et conservées les données des e-PV […] ainsi que les données contenues dans les annexes de ces e-PV », est la « banque de données centrale des procès-verbaux électroniques »[4].

L'article 100/6 du Code pénal social est consacré à cette banque de données, laquelle reprend les données contenues dans les procès-verbaux électroniques et dans leurs annexes.

2.1.3. Banque de données GINAA

La banque de données GINAA (*Geïntegreerde Informatica-applicaties Administratieve Geldboetes*) est, selon l'article 16, 19°, du Code pénal social, « la banque de

1. Article 100/2 C. pén. soc. ; M. Morsa, *op. cit.*, p. 174 ; *Manuel e-PV*, *op. cit.*, p. 3.
2. *Ibid.*, p. 103.
3. *Ibid*.
4. M. Morsa, *op. cit.*, p. 178.

données de l'administration compétente, qui contient les données relatives aux missions qui lui sont attribuées dans ou en vertu du livre 1er ».

Dans la définition, l'« administration compétente » vise la Direction des amendes administratives, d'une part, est en charge « de la poursuite, par voie d'une amende administrative, des employeurs qui commettent une infraction à la législation »[1] sociale et, d'autre part, conformément à l'article 70 du Code pénal social, peut « infliger des amendes administratives en cas d'infraction à la législation sociale lorsque l'auditeur du travail renonce aux poursuites pénales »[2].

La banque de données GINAA, dont l'existence est encadrée par l'article 100/11 du Code pénal social, constitue une banque de données développée en interne à la DAA et que cette dernière utilise dans la gestion de ses dossiers[3]. Elle est complètement « indépendante de la banque de données e-PV »[4].

Elle contient toutes les données structurées des e-PV en format XML ainsi que les e-PV accompagnés de leurs annexes en format PDF[5]. Ces informations sont mises à jour quotidiennement, afin que les fonctionnaires compétents puissent infliger « des amendes administratives dans le cadre des procès-verbaux »[6]. En effet, il est essentiel de prévoir, entre les autorités judiciaires et la DAA, un échange « d'informations sur les amendes administratives infligées et sur les poursuites pénales éventuelles qui ont été entamées dans le cadre d'un PV déterminé »[7].

Un transfert s'opère évidemment entre la banque de données e-PV et la banque de données GINAA, par « voie électronique, à l'intervention de la Banque-Carrefour de la sécurité sociale »[8].

2.2. Processus de rédaction de l'e-PV

Il existe une obligation légale, prévue à l'article 100/2 du Code pénal social, en vertu de laquelle les inspecteurs sociaux sont tenus de dresser les procès-verbaux de constatation d'infractions de manière électronique.

Concrètement, après avoir constaté une infraction au Code pénal social, un inspecteur déterminé se connecte à l'application e-PV et complète un formulaire en ligne.

1. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, délibération n° 10/068 du 7 septembre 2010, p. 3.
2. Projet de loi-programme, *Doc. parl.*, Sénat, 2011-2012, n° 1545/5, p. 4.
3. Justification du budget général des dépenses pour l'année budgétaire 2015, *op. cit.* p. 15 ; projet de loi-programme, *Doc. parl.*, Sénat, 2011-2012, n° 1545/5, p. 11.
4. Projet de loi-programme, *Doc. parl.*, Sénat, 2011-2012, n° 1545/5, p. 11.
5. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, *op. cit.*, p. 3.
6. Projet de loi-programme, *op. cit.*, p. 11.
7. *Ibid.*
8. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, *op. cit.*, p. 4.

Une série de champs doit obligatoirement être complétée :

– l'identité des personnes concernées par le procès-verbal (les auteurs et coauteurs éventuels de l'infraction, la personne civilement responsable, les travailleurs ou d'autres personnes) ;
– l'infraction réalisée ainsi que son lieu, sa date et son heure ;
– des informations concernant la constatation de l'infraction ;
– un exposé des faits ;
– des informations complémentaires telles que les circonstances particulières ou les éventuels antécédents.

Des annexes, notamment des photos, des auditions ou des documents scannés, peuvent également être jointes au procès-verbal.

Après avoir indiqué les destinataires de l'original du procès-verbal (à savoir une autorité judiciaire, en principe l'auditeur du travail ou le procureur du Roi) et des copies (au contrevenant, le cas échéant, au civilement responsable et à la DAA) et vérifié si toutes les rubriques obligatoires ont été complétées, l'inspecteur peut cliquer sur l'icône permettant de signer électroniquement l'e-PV. Le procès-verbal sous format PDF apparaît, numéroté de manière définitive, et l'inspecteur peut alors le signer par le biais de sa carte d'identité électronique[1]. Une fois signé, l'e-PV ne peut plus être modifié ou supprimé.

Ensuite, les e-PV sont imprimés, signés à la main et transmis par courrier ordinaire à l'autorité judiciaire et, par courrier recommandé, au contrevenant et, éventuellement, au civilement responsable[2]. La DAA quant à elle reçoit le PV par voie électronique.

Précisons qu'il est prévu que, dans le futur, l'e-PV soit transmis à l'ensemble destinataires de manière électronique[3].

Finalement, la preuve de l'envoi recommandé d'une copie du procès-verbal électronique au contrevenant est ajoutée au procès-verbal électronique.

2.3. Règles applicables en matière d'accès aux e-PV

Tout comme pour le processus de rédaction de l'e-PV, un système particulier, fondé respectivement sur l'article 100/10 et l'article 100/12 du Code pénal social, a été instauré au sujet de la consultation de la banque de données e-PV et de la banque de

1. *Manuel e-PV*, *op. cit*., pp. 10 et s.
2. Projet de loi-programme, *Doc. parl*., Sénat, 2011-2012, n° 1545/5, p. 4.
3. Rapport annuel de la Direction générale Contrôle du bien-être au travail, 2007, www.emploi.belgique.be.

données GINAA. En outre, des dispositions communes aux deux banques de données sont reprises à l'article 100/13 du Code.

2.3.1. Accès à la banque de données e-PV

Le fait d'octroyer à plusieurs services d'inspection le droit d'accéder à la banque de données e-PV leur permet d'avoir une vue sur les constatations des autres services d'inspection de manière rapide, simple et structurée. Grâce à cela, ils sont capables « de traiter leurs (propres) dossiers en connaissance de cause et de préparer leurs contrôles en ayant recours aux constatations antérieures de leurs collègues »[1].

Les règles d'accès à cette banque de données sont complexes et diffèrent en vertu de plusieurs paramètres.

Tout d'abord, il convient de distinguer l'hypothèse du procès-verbal électronique en cours de rédaction de celui qui est signé et, dès lors, définitif.

Un e-PV en cours de rédaction peut être consulté par l'inspecteur-auteur de l'e-PV (le verbalisant) et par les autres membres de son service d'inspection. Par contre, seul le verbalisant a la possibilité de le modifier, de le compléter, voire de le supprimer[2].

En ce qui concerne le régime d'accès au procès-verbal définitif, il diffère selon que le procès-verbal est issu du service de l'inspecteur désirant le consulter ou s'il a été dressé dans un autre service d'inspection. En tout état de cause, le procès-verbal signé ne peut être modifié, complété ou supprimé[3].

D'une part, un inspecteur a accès à tous les procès-verbaux de son service d'inspection.

D'autre part, au sujet des procès-verbaux rédigés par d'autres services d'inspection, il faut distinguer si l'e-PV a été dressé de la propre initiative de l'inspecteur ou en exécution d'un mandat judiciaire.

En effet, alors que les données des e-PV dressés à la suite d'une apostille ne peuvent pas être librement consultées, un inspecteur peut avoir accès aux données du procès-verbal dressé de la propre initiative d'un autre inspecteur, en vertu de l'article 100/10, § 1er, du Code pénal social.

1. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, délibération n° 04/032 du 5 octobre 2004 concernant la consultation des banques de données sociales par les services d'inspection sociale, p. 33.
2. *Manuel e-PV, op. cit.*, pp. 70 et 71.
3. *Ibid.*, p. 72.

Une telle consultation se réalise en deux temps. Premièrement, l'inspecteur a accès aux données de référence, qui sont reprises à l'article 100/10, § 1er, du Code pénal social[1]. Dans un second temps, si, sur la base de ces données, l'e-PV présente un intérêt pour lui dans l'exercice de la surveillance, l'inspecteur pourra avoir accès aux autres informations contenues dans l'e-PV. Il disposera alors du procès-verbal sous format PDF, accompagné de ses annexes[2], conformément à l'article 100/10, § 2, du Code pénal social.

Par contre, lorsque l'e-PV a été rédigé à la suite d'une apostille, à savoir sur ordre d'un magistrat (auditeur du travail, procureur du roi ou juge d'instruction), toutes les données contenues dans ce procès-verbal ne sont pas librement consultables. En effet, les inspecteurs peuvent accéder aux données de référence de l'e-PV, mais pas aux autres données (et, dès lors, pas à l'e-PV sous format PDF et à ses annexes)[3]. Pour pouvoir consulter l'e-PV dans son entièreté, l'inspecteur doit contacter le magistrat concerné afin de demander l'autorisation d'accès (art. 100/10, § 2, *in fine*, C. pén. soc.). Une fois cette autorisation obtenue, l'inspecteur peut se tourner vers l'auteur de l'e-PV et solliciter l'envoi d'une copie de l'e-PV dans son entièreté.

Notons encore qu'une autorisation préalable accordée par la section Sécurité sociale du Comité sectoriel de la Sécurité sociale et de la Santé est nécessaire pour avoir accès aux données de référence des e-PV rédigés par les autres services d'inspection. Néanmoins, celle-ci n'est pas nécessaire pour les données des e-PV dressés par son propre service (art. 100/10, §§ 1er et 2, alinéa 2, C. pén. soc.).

En exception à ces principes, un e-PV peut être placé « sous embargo » par le ministère public[4], conformément à l'article 100/10, § 6, du Code. Il s'agit d'un procès-verbal « dont l'existence ne peut être connue tant que l'instruction pénale est en cours »[5]. Le magistrat retarde alors l'accès aux données contenues dans ce procès-verbal lorsque et tant que le magistrat compétent est d'avis que cet accès peut constituer un danger pour l'exercice de l'action pénale ou pour la sécurité d'une per-

1. Il s'agit de :
   (i) la date d'établissement du procès-verbal ;
   (ii) le numéro du procès-verbal ;
   (iii) l'indication du fait qu'il s'agit d'un procès-verbal établi d'initiative par le verbalisant ou en exécution d'un devoir prescrit par une autorité judiciaire ;
   (iv) le service auquel appartient le fonctionnaire verbalisant ;
   (v) le nom du fonctionnaire verbalisant ;
   (vi) l'identité et l'adresse du domicile ou du siège social de toute personne suspectée d'être (co)auteur d'une infraction ;
   (vii) l'identité et l'adresse du domicile ou du siège social de toute personne qui est tenue civilement responsable pour une infraction ;
   (viii) le cas échéant, le nom et le numéro d'identification à la sécurité sociale de tout travailleur ou de toute personne concerné(e) ou considéré(e) comme étant concerné(e) par une infraction ;
   (ix) la qualification de l'(des) infraction(s) constatée(s).
2. *Manuel e-PV, op. cit.*, p. 73.
3. *Ibid.*
4. *Ibid.*, p. 74.
5. *Ibid.*

sonne. Un procès-verbal électronique sous embargo ne peut être consulté que par son auteur.

Des dispositions spécifiques du Code pénal social sont consacrées aux autres catégories d'acteurs ayant accès aux données contenues dans la banque de données e-PV.

Primo, le paragraphe 3 de l'article 100/10 du Code pénal social concerne les membres du personnel de la Direction des amendes administratives du SPF ETCS. Moyennant l'autorisation de la section Sécurité sociale du Comité sectoriel de la Sécurité sociale et de la Santé, ils ont accès à toutes les données de la banque de données e-PV (données de référence et autres), pour autant que ces données présentent un intérêt pour eux dans l'exercice de leur mission légale.

Secundo, en vertu de l'article 100/10, § 4, du Code pénal social, le ministère public près des cours et tribunaux et les juges d'instruction ont accès à toutes les données de la banque de données e-PV, dans le cadre de sa mission légale. À cet égard, notons qu'une autorisation du Comité sectoriel de la Sécurité sociale et de la Santé n'est pas requise à la suite d'une demande expresse du Collège des procureurs généraux, et ce, afin que soit respecté le principe de la séparation des pouvoirs[1].

Tertio, l'article 100/10, § 5, du Code pénal social prévoit la possibilité, pour le Comité sectoriel de la Sécurité sociale et de la Santé, section Sécurité sociale, d'étendre les droits d'accès aux données de la banque e-PV à d'autres catégories d'acteurs de la lutte contre le travail illégal et la fraude sociale, et en indique les modalités.

Le mécanisme mis en place concernant la consultation d'un e-PV prévoit également que chaque consultation doit être justifiée – l'inspecteur doit indiquer les raisons de sa consultation dans un champ spécifique – et enregistrée. Des contrôles *a posteriori* sont réalisés par un fonctionnaire chargé de la sécurité, qui vérifie le caractère justifié des consultations. Au surplus, la Commission de la protection de la vie privée est désignée, par l'article 100/9 du Code pénal social, comme organe de contrôle et doit vérifier la légalité des consultations effectuées[2].

Pour conclure sur ce point, il convient de préciser que l'autorisation du Comité sectoriel, exigée par les divers articles du Code pénal social énoncés ci-dessus, a été donnée par une délibération du Comité sectoriel de la Sécurité sociale et de la Santé n° 04/032 concernant la consultation des banques de données sociales par les services d'inspection sociale[3]. Le Comité sectoriel a ainsi autorisé les services d'inspec-

1. Projet de loi-programme, *Doc. parl.*, Sénat, 2011-2012, n° 1545/5, pp. 4 et 5.
2. *Manuel e-PV*, *op. cit.*, p. 74.
3. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, délibération n° 04/032 du 5 octobre 2004 modifiée le 1er septembre 2009, le 9 novembre 2010, le 6 mars 2012, le 3 décembre 2013, le 4 février 2014, le 6 mai 2014 et le 3 juin 2014, concernant la consultation des banques de données sociales par les services d'inspection sociale.

tion concernés à consulter les données de la banque de données e-PV, « sous l'expresse condition du respect des conditions »[1] indiquées dans la délibération, principalement en matière de sécurité et d'exigences techniques.

2.3.2. Accès à la banque de données GINAA

L'accès à la banque de données GINAA est prévu par l'article 100/12 du Code pénal social, qui indique que, d'une part, un arrêté royal désignera les catégories de personnes qui y auront accès « pour autant que cela soit nécessaire à l'exercice de leurs missions légales » et, d'autre part, que l'accès aux données n'est possible qu'après avoir reçu l'autorisation de la section Sécurité sociale du Comité sectoriel de la Sécurité sociale et de la Santé.

À notre connaissance, l'arrêté royal n'a pas encore été pris et une telle autorisation du Comité sectoriel de la Sécurité sociale et de la Santé n'a pas encore été octroyée.

Pour l'instant, seuls les membres de la DAA ont accès à cette banque de données ainsi que certaines personnes des services d'inspection du SPF ETCS.

2.3.3. Dispositions communes aux deux banques de données

Suivant l'article 100/13 du Code pénal social, chaque entité qui est autorisée à accéder à l'une ou l'autre banque de données est tenue d'établir une liste mise à jour continuellement des personnes qu'elle a désignées afin d'exercer ce droit d'accès.

Toutes les personnes qui ont accès à ces banques de données doivent prendre les mesures nécessaires afin de garantir non seulement le caractère confidentiel des données à caractère personnel contenues dans ces banques de données, mais aussi l'utilisation de ces données uniquement en vue des finalités précisées dans le Code pénal social et explicitées au point 3.1.2.2.A ci-dessous.

3. Défis juridiques

3.1. Vie privée et protection des données à caractère personnel

Dans le cadre de l'utilisation du système e-PV, des données à caractère personnel de milliers de citoyens sont collectées, enregistrées, conservées et utilisées par les diffé-

1. *Ibid.*, p. 42.

rents services d'inspection autorisés. Dès lors, les régimes juridiques de la protection de la vie privée et de la protection des données à caractère personnel trouvent à s'appliquer[1].

Dans un avis n° 05/2012, la Commission de la protection de la vie privée a été amenée à se prononcer sur l'avant-projet relatif aux ajouts des articles 100/1 à 100/13 dans le Code pénal social. Cet avis constitue une source intéressante dans le cadre de la confrontation entre la législation consacrée à l'e-PV et la réglementation relative à la vie privée et à la protection des données à caractère personnel.

3.1.1. e-PV et droit au respect de la vie privée

En droit belge, l'article 22 de la Constitution consacre le sacro-saint principe du droit au respect de la vie privée et familiale de chaque citoyen. Cette disposition a été interprétée par la jurisprudence, et notamment celle de la Cour constitutionnelle, ainsi que par la section de législation du Conseil d'État, et il en a été déduit une obligation, pour le législateur, non seulement de déterminer « les éléments essentiels des traitements des données menés dans l'administration »[2], mais également de le faire dans une loi claire et précise[3].

Parmi les éléments essentiels des traitements devant être fixés dans l'instrument législatif doivent se retrouver le type de données collectées et stockées dans une base de données, la durée de cette conservation ou, encore, les institutions disposant du droit d'accès à ces informations[4].

Ainsi, dans son avis du 8 février 2012, la Commission de la protection de la vie privée a rappelé, au sujet des banques de données e-PV et GINAA, que « l'article 22 de la Constitution requiert […] une intervention légale formelle pour mettre en place et/ou encadrer des banques de données publiques d'une telle ampleur »[5].

Bien que cette obligation d'intervention légale ne soit pas respectée en toutes circonstances lors de l'instauration de nouveaux traitements de données dans l'administration[6], dans le cas d'espèce, une loi, qui reprend les éléments exigés par la jurisprudence et la doctrine, a bien été adoptée. Il s'agit de la loi-programme du 29 mars 2012, qui a inséré les articles 100/1 à 100/13 dans le Code pénal social.

1. E. Degrave, « Le-gouvernement et la protection de la vie privée », *C.D.P.K.*, 2013, p. 234.
2. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 309.
3. *Ibid.*, pp. 178 et 309.
4. E. Degrave, « Le-gouvernement et la protection de la vie privée », *op.cit.*, 2013, p. 238.
5. C.P.V.P., avis n° 05/2012 du 8 février 2012, p. 3.
6. E. Degrave, « Le-gouvernement et la protection de la vie privée », *op.cit.*., 2013, p. 238.

3.1.2. e-PV et protection des données à caractère personnel

Outre le droit au respect de la vie privée, la collecte et l'utilisation des informations personnelles au sujet des citoyens doivent être réalisées conformément au prescrit de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après, « loi vie privée » ou « LVP »). Cette dernière s'applique, en principe, à tout traitement de données à caractère personnel, qu'ils soient réalisés par des acteurs du secteur privé ou public[1].

Après avoir évoqué les éléments devant nécessairement être rencontrés pour que s'applique la loi du 8 décembre 1992, nous reviendrons sur les grands principes sous-tendant le régime de protection des données à caractère personnel.

3.1.2.1. Application de la législation

La loi du 8 décembre 1992 n'intervient que si la mise en place d'un système engendre un traitement des données à caractère personnel de personnes physiques. Doit alors être désigné un responsable de ce traitement, qui sera tenu d'assurer le respect d'une série d'obligations.

A. Traitement de données à caractère personnel

À la vue du système e-PV, il apparaît incontestablement que des données à caractère personnel sont impliquées. D'ailleurs, le Code pénal social cite explicitement les personnes dont les données sont reprises dans les banques de données e-PV et GINAA.

D'une part, l'article 100/6, alinéa 4, du Code pénal social indique que la banque de données e-PV contient « des données qui sont reprises dans le modèle d'e-PV […], à propos des personnes suivantes :

1° toute personne suspectée d'être (co)auteur d'une infraction ;
2° toute personne qui est civilement tenue responsable pour une infraction ;
3° tout travailleur ou personne qui est concerné ou considéré comme étant concerné par une infraction ;
4° toute autre personne mentionnée dans l'e-PV dont la reprise des données dans l'e-PV est nécessaire pour une bonne compréhension des faits constatés dans l'e-PV ».

La notion de « données qui sont reprises dans le modèle d'e-PV » n'est pas définie de manière explicite dans le Code pénal social. Néanmoins, divers articles citent des données contenues dans les e-PV. Ainsi, l'article 100/10, § 1er, énonce une série de

1. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 254.

données de référence et l'article 100/10, § 2, évoque des « données autres que celles mentionnées dans le § 1er […] y compris les constatations ». D'après la Commission de la protection de la vie privée, ces autres données consistent en des « informations sur l'infraction constatée aux dispositions prévues par le Code pénal social, notamment la mention de l'identité des parties impliquées, leur statut et les constatations effectuées »[1].

D'autre part, il est prévu, à l'article 100/11, alinéa 3, du Code pénal social, que la banque de données GINAA « contient les données déterminées par le Roi à propos de :

1° toute personne suspectée d'être (co)auteur d'une infraction ;
2° toute personne à qui une amende administrative peut être infligée ;
3° tout travailleur ou personne qui est concerné ou considéré comme étant concerné par une infraction ».

Nous avons précédemment exposé que cette banque de données contient toutes les données structurées des e-PV, ainsi que les procès-verbaux eux-mêmes en format PDF et accompagnés de leurs annexes.

Ensuite, il convient de se demander si des traitements ont lieu sur les données à caractère personnel des citoyens. Une réponse positive doit être accordée à cette question. En effet, les données sont collectées ou rapatriées d'autres bases de données, avant d'être stockées, éventuellement modifiées, mises à jour ou supprimées, et surtout consultées et utilisées.

Par ailleurs, la loi vie privée, en son article 8, accorde un statut particulier, accompagné d'un régime plus protecteur, à une série de données qualifiées de « sensibles ». En l'espèce, il s'agit des « données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté » (art. 8, § 1er, LVP). Dans un souci de simplification, ces données sont usuellement dénommées les « données judiciaires ». Or, l'article 8 de la loi du 8 décembre 1992 prévoit l'interdiction du traitement des données judiciaires. La disposition poursuit en énumérant une série d'exceptions à ce principe. Ainsi, est notamment autorisé le traitement de ces données effectué « lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance » (art. 8, § 2, b, LVP). Comme le pointe la Commission de la protection de la vie privée, cette exception joue dans le cas du système e-PV, puisque le traitement est nécessaire à la réalisa-

1. C.P.V.P., avis n° 05/2012 du 8 février 2012, p. 6.

tion des finalités déterminées dans le Code pénal social[1]. Le traitement des données judiciaires est dans ce cas, autorisé.

B. Responsable du traitement

Le législateur a pris le soin, dans le Code pénal social, de définir le responsable des traitements opérés dans le cadre de la banque de données e-PV et dans le cadre de la banque de données GINAA.

Ainsi, relativement à cette dernière, il est inscrit, à l'article 100/11 du Code qu'« en ce qui concerne la banque de données GINAA […], le Service public fédéral Emploi, Travail et Concertation sociale est le responsable pour le traitement des données ».

Quant à la banque de données e-PV, l'article 100/6, alinéa 2, prévoit que « l'État belge, représenté par le ministre compétent pour l'[E]mploi, par le ministre compétent pour les [A]ffaires sociales et par le ministre compétent pour la [J]ustice, est responsable pour le traitement » des données impliquées.

3.1.2.2. Grands principes

Pour être admissible et conforme à la loi du 8 décembre 1992, un traitement de données à caractère personnel doit respecter des principes fondamentaux. Ainsi, le traitement doit, conformément au principe de finalité, poursuivre une ou plusieurs finalités déterminées, explicites et légitimes. De plus, le principe de la proportionnalité exige que les données impliquées, tout comme le traitement mis en œuvre, soient nécessaires et appropriées[2]. Enfin, le principe de la transparence est également central lors de tout traitement de données à caractère personnel.

A. Finalité

La finalité d'un traitement est la raison pour laquelle ledit traitement est réalisé[3]. L'article 4, § 1er, 2°, de la LVP prévoit que les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités […] ».

Alors que le Code pénal social reprend de manière expresse les finalités poursuivies par les banques de données e-PV et GINAA, un raisonnement plus approfondi est

1. C.P.V.P., avis n° 05/2012 du 8 février 2012, pp. 3 et 4.
2. Article 4 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993. ; E. Degrave, « Le-gouvernement et la protection de la vie privée », *op.cit.*, p. 239 ; C. De Terwangne, « Analyse détaillée de la loi de protection des données et de son arrêté d'exécution », *Vie privée et données à caractère personnel*, Bruxelles, Politeia, p. 67.
3. C. De Terwangne, « Analyse détaillée de la loi de protection des données et de son arrêté d'exécution », *op. cit.*, p. 52.

nécessaire afin de déterminer quelle finalité est poursuivie par le transfert des données à partir de et vers ces deux banques de données.

Premièrement, pour la banque de données e-PV, l'article 100/6, alinéa 3, du Code pénal social liste trois finalités :

« 1° la collecte de l'information utile pour permettre aux acteurs de la lutte contre le travail illégal et la fraude sociale de combattre de manière adéquate le travail illégal et la fraude sociale ;
2° la collecte de l'information utile pour permettre aux acteurs de la lutte contre le travail illégal et la fraude sociale d'effectuer leurs missions légales ;
3° l'élaboration de statistiques internes et externes ».

Deuxièmement, les finalités énoncées à l'article 100/11, alinéa 2, du Code pénal social concernent la banque de données GINAA :

« 1° la collecte de l'information qui est utile pour permettre à l'administration compétente (soit la DAA) d'exercer les missions qui lui sont attribuées dans ou en vertu du Livre I^er^ [du Code pénal social] ;
2° la collecte de l'information relative à la poursuite des infractions qui est utile pour permettre aux acteurs de la lutte contre le travail illégal et la fraude sociale d'exercer leurs missions légales ;
3° la collecte de l'information relative à la poursuite des infractions qui est utile pour permettre aux acteurs de la lutte contre le travail illégal et la fraude sociale de combattre de manière adéquate le travail illégal et la fraude sociale ;
4° l'élaboration de statistiques internes et externes ».

Après avoir repris ces dispositions, la Commission de la protection de la vie privée se contente de noter que « ces finalités sont déterminées, explicites et légitimes au sens de l'article 4, § 1^er^, 2°, de la LPVP »[1].

Nous pouvons cependant nous interroger sur le caractère *déterminé* de ces finalités en vertu duquel les finalités doivent être précises[2]. En l'espèce, les finalités énoncées dans la loi sont extrêmement floues et ne semblent pas remplir la condition de la finalité déterminée.

Troisièmement, concernant les flux de données à partir de et vers les deux banques de données, il convient d'analyser les articles 14 et 15 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (ci-après, « la loi BCSS »), puisque, d'une part, le transfert s'opère par voie électronique, à l'intervention de la Banque-carrefour de la sécurité sociale et, d'autre part,

1. C.P.V.P., avis n° 05/2012 du 8 février 2012, p. 4.
2. C. De Terwangne, « Analyse détaillée de la loi de protection des données et de son arrêté d'exécution », *op. cit.*, p. 52.

les données reprises dans ces banques de données sont des données sociales à caractère personnel. En effet, de telles données sont des données sociales – c'est-à-dire des « données nécessaires à l'application de la sécurité sociale »[1] – et à caractère personnel, car elles concernent « une personne physique identifiée ou identifiable »[2].

L'article 15, § 1er, alinéa 1er, de la loi précitée impose que « toute communication dans le réseau de données sociales à caractère personnel, par la Banque-carrefour ou les institutions de sécurité sociale » soit autorisée par le Comité sectoriel de la Sécurité sociale et de la Santé, section Sécurité sociale.

Conformément à cette disposition, le flux de données partant de la banque de données e-PV vers la banque de données GINAA a été approuvé par le Comité sectoriel de la Sécurité sociale et de la Santé, dans sa délibération n° 10/068 du 7 septembre 2010 relative à la communication de données à caractère personnel de la banque de données à caractère personnel e-PV par certains services d'inspection au SPF ETCS en vue d'infliger des amendes administratives[3].

Dans la délibération précitée, le Comité sectoriel a analysé le mécanisme de la communication des données à caractère personnel « relatives aux personnes concernées par la constatation d'une infraction à la législation sociale »[4] de la banque de données e-PV à la banque de données GINAA.

Ainsi, il a exposé que la finalité de ce transfert était légitime, puisque cette finalité est l'exécution des missions de la Direction des amendes administratives, telles que décrites dans la loi du 31 juin 1971 et dans l'arrêté royal du 1er avril 2007[5]. Ensuite, il faut se demander si les caractères *déterminé* et *explicite* sont également reconnus aux finalités. À la lecture de ces deux normes, nous pouvons considérer que ces conditions sont remplies.

Dès lors, il ressort de la délibération du Comité sectoriel précité que les finalités poursuivies par l'échange des données entre la banque de données e-PV et la banque de données GINAA respectent l'article 4, § 1er, 2°, de la loi du 8 décembre 1992.

Pour conclure, on peut s'interroger sur la raison suivant laquelle les finalités poursuivies par les deux banques de données ont été précisées dans le Code pénal social

1. Article 2, 4°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990.
2. Article 2, 6°, de la loi du 15 janvier 1990.
3. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, délibération n° 10/068 du 7 septembre 2010, p. 2.
4. *Ibid*.
5. Ces missions sont décrites dans la loi du 30 juin 1971 relative aux amendes administratives applicables en cas d'infraction à certaines lois sociales et dans l'arrêté royal du 1er avril 2007 portant exécution de la loi du 30 juin 1971 relative aux amendes administratives applicables en cas d'infraction à certaines lois sociales. Voy. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, délibération n° 10/068 du 7 septembre 2010, p. 4.

alors qu'il a été omis de définir celles par le transfert de données d'une banque de données à l'autre.

B. Proportionnalité

En plus des exigences liées à la finalité, tout traitement de données à caractère personnel doit respecter le principe de la proportionnalité qui s'applique tant aux données elles-mêmes qu'au traitement qui en est fait.

En vertu de ce principe, non seulement le traitement doit être légitime, c'est-à-dire nécessaire et opéré en respectant « un juste équilibre entre le but poursuivi et l'immixtion créée dans la vie privée des citoyens »[1], mais les données traitées doivent également être d'une certaine qualité[2].

Plus précisément, l'article 4, § 1er, 3°, de la loi du 8 décembre 1992 prescrit que les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

De par cette exigence de proportionnalité, il pèse sur le législateur l'obligation de déterminer les moyens de traitement mis à disposition des administrations[3].

Dans son rapport, la Commission de la protection de la vie privée a conclu que les données qui sont reprises dans les banques de données e-PV et GINAA, et qui ont été citées précédemment, sont conformes aux exigences de l'article 4, § 1er, 3°, de la LVP.

En outre, cet examen de la proportionnalité implique que soient analysés les traitements qui sont opérés sur les données.

Parmi toutes les opérations pouvant être réalisées sur les données contenues dans les banques de données, deux nous semblent plus délicates. Il s'agit, d'une part, des opérations d'accès et, d'autre part, du transfert des données entre les deux banques de données.

Au sujet de cette communication d'informations entre la banque de données e-PV et la banque de données GINAA, il est pertinent de revenir sur l'avis n° 10/068 du Comité sectoriel de la Sécurité sociale et de la Santé, section Sécurité sociale. Ce dernier a indiqué que les données communiquées par voie informatique, « à l'intervention de la Banque-Carrefour de la sécurité sociale, conformément à l'article 14 de

1. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 213.
2. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 226.
3. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 309.

la loi du 15 janvier 1990 »[1], étaient pertinentes et non excessives au regard de cette finalité.

Ensuite, au point 2.3 de cette contribution, nous avions exposé les règles d'accès aux deux banques de données e-PV et GINAA. Il convient maintenant d'analyser cette réglementation, et plus précisément le traitement qui consiste en la consultation de ces données, au regard du principe de la proportionnalité.

Premièrement, en ce qui concerne la banque de données e-PV, il a été exposé que seuls les membres du personnel habilités des services d'inspection sociale avaient accès aux données de référence des e-PV enregistrés dans la banque de données. Sur la base de ces données, ils peuvent ainsi vérifier si un procès-verbal particulier contient des informations présentant un intérêt pour eux dans l'exercice de leur mission de surveillance.

Deux hypothèses peuvent alors se présenter. Soit le procès-verbal ne présente pas d'intérêt légitime pour l'inspecteur et, dans ce cas, il n'y a aucune raison pour étendre l'accès aux autres données (le PDF de l'e-PV et les éventuelles annexes). Ainsi, l'accès dont il dispose respecte l'article 4, § 1er, 3°, de la LVP, en ce qu'il n'est pas excessif. Soit le procès-verbal est utile à l'inspecteur et il existe alors un intérêt légitime pour étendre l'accès aux autres données. Un tel accès est pertinent au sens de la disposition susmentionnée[2].

La Commission de la protection de la vie privée remarque que le régime légal de l'e-PV a prévu « de proportionner l'accès et les possibilités de traitement des membres du personnel habilités des services d'inspection sociale »[3], puisque, afin d'étendre cet accès aux données autres que les données de référence, il faut disposer d'un intérêt fonctionnel concret.

Trois autres mesures de protection peuvent également être soulignées. D'abord, il est exigé d'obtenir l'autorisation du Comité sectoriel de la Sécurité sociale et de la Santé avant de pouvoir accéder à ces autres données. Ensuite, dans l'hypothèse où un procès-verbal aurait été rédigé à la suite d'un mandat judiciaire, l'accès aux données autres que les données de référence est soumis à l'autorisation de l'autorité judiciaire concernée. Enfin, la Commission de la protection de la vie privée est désignée comme organe de contrôle.

Selon la Commission de la protection de la vie privée, l'ensemble de ces éléments participe à garantir que l'accès aux informations contenues dans la banque de données e-PV ne sera accordé que pour des données adéquates, pertinentes et non

1. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, délibération n° 10/068 du 7 septembre 2010, p. 4.
2. C.P.V.P., avis n° 05/2012 du 8 février 2012, p. 8.
3. *Ibid*.

excessives, dans le respect du prescrit de l'article 4, § 1er, 3°, de la loi du 8 décembre 1992.

Deuxièmement, relativement à la banque de données GINAA, la Commission de la protection de la vie privée considère qu'en raison de l'exigence d'autorisation par le Comité sectoriel de la Sécurité sociale et de la Santé, les règles prévues à l'article 100/13 du Code pénal social et développées précédemment garantissent « qu'un accès sera uniquement accordé à des données adéquates, pertinentes et non excessives de la banque de données GINAA, conformément à l'article 4, § 1er, 3°, de la loi vie privée »[1]. D'ailleurs, le Comité sectoriel de la Sécurité sociale et de la Santé, section Sécurité sociale a, dans son avis n° 10/068, exposé que l'accès aux données, dans cette banque de données, devait être restreint aux collaborateurs désignés de la DAA et qu'une liste mise à jour des collaborateurs concernés devait être détenue par cette institution, qui devra la transmettre au Comité sur simple demande[2].

C. Transparence

Parallèlement à ces deux grands principes, une exigence de transparence doit être respectée dans le cadre de l'e-gouvernement de manière générale.

La transparence, qui se définit comme « l'ensemble des obligations constitutionnelles et légales qui visent à permettre au citoyen de connaître et de comprendre l'organisation et le fonctionnement de l'administration »[3], se base sur une double source de règles : la transparence des traitements de données à caractère personnel et la transparence administrative.

En vertu de cette dernière, tout administré dispose du droit de « satisfaire sa curiosité légitime à l'égard de toutes les informations détenues par l'administration »[4].

La transparence des traitements de données à caractère personnel, qui nous intéresse dans le cadre de cette analyse, octroie aux citoyens la possibilité de prendre connaissance des données qu'un responsable de traitement détient à son sujet et des traitements réalisés sur les données le concernant[5]. Ce droit, qualifié de droit d'accès, est prévu à l'article 10 de la LVP.

Ce principe connaît cependant d'importantes limitations, précisées à l'article 3, §§ 4, 5 et 6, de la loi du 8 décembre 1992.

---

1. *Ibid*.
2. Comité sectoriel de la Sécurité sociale et de la Santé. Section Sécurité sociale, délibération n° 10/068 du 7 septembre 2010, p. 4.
3. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit*., p. 313.
4. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit*., p. 313.
5. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit*., p. 313.

En effet, diverses autorités publiques sont dispensées du respect des obligations de transparence notamment pour les traitements de données effectués dans le cadre de l'exercice de leurs missions de police judiciaire[1] ou de police administrative (qui ont été désignées par un arrêté royal délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée)[2].

En vue de démontrer que le système e-PV remplit cette exigence de transparence malgré l'absence de droit d'accès direct ci-dessus évoqué, divers éléments sont mis en avant par la Commission de la protection de la vie privée.

Cette dernière indique, dans un premier temps, que le fait d'avoir précisé les aspects centraux des e-PV et des deux banques de données dans une loi formelle, publiée au *Moniteur belge*, participe à la transparence de manière générale[3].

Dans un second point, la Commission met l'accent sur la possibilité dont disposent les personnes concernées de s'adresser à elle afin de mettre en œuvre leur droit d'accès, de rectification d'informations inexactes et de suppression des données ou, encore, « d'interdiction d'utilisation de données interdites ou de données non pertinentes »[4], et ce, conformément à l'article 13 de la loi du 8 décembre 1992. Cette disposition consacre un droit d'accès indirect et s'applique dès lors que les traitements opérés sur les données sont gérés par des autorités publiques en vue de l'exercice de leurs missions de police judiciaire. En outre, la Commission de la protection de la vie privée dispose d'un pouvoir de contrôle des traitements de données effectués en vertu de l'article 32 de la LVP et de l'article 100/9 du Code pénal social[5].

Or le droit d'accès indirect nous apparaît comme faible, puisqu'en réalité, tel que le prévoit l'article 13 de la LVP, la Commission de la protection de la vie privée, après avoir effectué un contrôle, « communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires » sans lui transmettre plus d'informations. Ainsi, par la mise en œuvre de cet article, la personne concernée « délègue entièrement son droit d'accès à la Commission de la protection de la vie privée et n'exerce plus aucun droit elle-même »[6].

Dans un troisième et dernier point, la Commission indique que, dans le cadre de la procédure *amende administrative*, la personne concernée dispose du droit d'accéder

1. Article 3, § 5, 1°, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
2. Article 3, § 5, 3°, de la loi du 8 décembre 1992.
3. C.P.V.P., avis n° 05/2012 du 8 février 2012, p. 10.
4. *Ibid*.
5. *Ibid*.
6. C. De Terwangne, « Analyse détaillée de la loi de protection des données et de son arrêté d'exécution », *op. cit.*, p. 96.

à son dossier repris dans la banque de données GINAA, sur la base de l'article 79 du Code pénal social[1], en vue d'assurer le respect des droits de la défense.

En conclusion, il est compréhensible en ce qui concerne les données judiciaires, un juste équilibre doive être trouvé entre, d'une part, les droits de la personne concernée et, d'autre part, les impératifs « tout aussi légitimes de la recherche ou de la poursuite des infractions »[2].

3.2. Valeur juridique de l'e-PV

En droit belge, la qualification d'un document en tant qu'original s'apprécie selon le critère de la signature dudit document. Au regard du droit de la preuve, « l'original est synonyme d'*écrit signé* » en Belgique[3] et un tel écrit est nécessaire, en droit civil, afin de prouver une obligation dont le montant est supérieur à 375 euros ou pour prouver outre un autre écrit signé. L'écrit signé figure donc en bonne place dans la hiérarchie des modes de preuve. La doctrine s'attache à considérer que l'original désigne « l'écrit revêtu d'une signature, qu'il soit établi par des personnes privées ou par un officier public »[4].

Dès lors, la signature est le seul critère existant pour pouvoir qualifier un document d'original en termes de preuve[5].

3.2.1. e-PV et signature électronique

Parmi les dispositions relatives à l'e-PV figurant dans le Code pénal social, l'article 100/3 requiert une attention particulière en ce qu'il prévoit une dérogation à l'article 7 de loi du 10 juillet 2006 relative à la procédure par voie électronique. L'article 7 de cette loi, qui s'inscrivait dans le cadre du projet Phénix, stipule que, « chaque fois qu'une disposition légale prévoit la signature d'une pièce de la procédure et qu'il s'agit d'une pièce électronique, celle-ci est pourvue de la signature qualifiée […]. Cette signature qualifiée est assimilée à une signature manuscrite »[6]. Cet article n'est toujours pas entré en vigueur. L'entrée en vigueur de cet article n'a pas encore eu lieu mais est prévue pour le 1er janvier 2017.

1. Article 79 C. pén. soc. : « L'administration compétente met à la disposition du contrevenant ou de son avocat le dossier relatif aux infractions pouvant donner lieu à l'application de l'amende administrative afin qu'il le consulte au greffe et elle l'autorise, sur demande, à prendre la copie des pièces du dossier. L'article 460*ter* du Code pénal est applicable au contrevenant qui est assimilé à l'inculpé en vue de l'application de cette disposition.
Les frais des copies sont à charge du contrevenant. Le tarif en est établi par le Roi. »
2. C. De Terwangne, « Analyse détaillée de la loi de protection des données et de son arrêté d'exécution », *op. cit.*, p. 96.
3. M. Demoulin et S. Soyez, *L'authenticité, de l'original papier à la copie numérique*, www.unesco.org, p. 3.
4. *Ibid.*, p. 3.
5. J. Larrieu, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? – Contribution à l'étude juridique des notions d'écriture et de signature », *Cah. Dr. Inf.*, 1988, p. 13.
6. Article 7 de la loi du 10 juillet 2006 relative à la procédure par voie électronique, *M.B.*, 7 septembre 2010.

Pour déterminer ce que l'on entend par « signature qualifiée », il y a lieu de se référer à l'article 2, 2° et 4°, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification[1]. Il s'agit, en fait, d'une signature électronique avancée[2] qui doit être certifiée par un certificat qualifié[3].

Or l'article 100/3 du Code pénal social prévoit que l'e-PV est signé par son auteur ou ses auteurs de manière électronique au moyen de la signature électronique qui est créée par la carte d'identité électronique. On se détache ici des notions habituellement retenues en matière de signature électronique pour préconiser l'utilisation d'une technologie en particulier. On ne parle ni de signature avancée ni de signature qualifiée, mais uniquement de signature réalisée au moyen de l'e-ID.

Le Roi peut néanmoins prévoir que l'e-PV soit signé de manière électronique au moyen d'un autre système, du moment que celui-ci permet de déterminer l'identité du signataire et l'intégrité de l'e-PV signé avec des garanties suffisantes[4]. Cette faculté a été initialement prévue dans le but d'éviter l'article 100/3 du Code pénal social relatif à la signature électronique ne devienne obsolète si le système de signature au moyen de l'e-ID venait à disparaître. Toutefois, l'usage de la signature électronique au moyen de l'e-ID est de plus en plus répandu en Belgique. La puce intégrée au sein de la carte d'identité permet au citoyen de s'identifier électroniquement et d'apposer sa signature sur des documents électroniques grâce aux certificats d'authentification et de signature présents sur celle-ci. Le certificat d'authentification permet de confirmer l'identité de la personne lors de la connexion à un site Web tandis que le certificat de signature fait en sorte que l'intéressé puisse apposer sa signature électronique.

La signature d'un document au moyen de l'e-ID est considérée comme étant une signature électronique qualifiée[5]. Ce type de signature permet d'attester que le document émane bien de la personne identifiée, qu'il n'a pas été modifié une fois la signature apposée et que la signature a été générée au moyen d'un certificat qualifié.

1. Article 2 de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001.
2. Une signature électronique avancée au sens de l'article 2, 2°, de la loi du 9 juillet 2001 n'est autre qu'une « donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :
   a) être liée uniquement au signataire ;
   b) permettre l'identification du signataire ;
   c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
   d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée ».
3. Au sens de la loi du 9 juillet 2001, il s'agit d'un « certificat qui satisfait aux exigences visées à l'annexe I de la présente loi et qui est fourni par un prestataire de services de certification satisfaisant aux exigences visées à l'annexe II de la présente loi ».
4. Article 100/3, § 1er, alinéa 2, C. pén. soc.
5. Rapport de la Cour des comptes sur la carte d'identité électronique transmis à la Chambre des représentants, Bruxelles, novembre 2012, p. 46.

Il est dès lors difficile de comprendre en quoi l'article 100/3 du Code pénal social « déroge » à l'article 7 de la loi du 10 juillet 2006. Le choix de ce vocable paraît inopportun.

Une des raisons de cette précision semble toutefois pouvoir être trouvée dans les travaux préparatoires : « Cette dérogation à l'article 7 de la loi du 10 juillet 2006 relative à la procédure par voie électronique est nécessaire maintenant que la signature électronique avec l'e-ID peut désormais être considérée comme une signature électronique avancée réalisée avec un certificat qualifié, mais l'e-ID elle-même n'a pas encore été jusqu'à présent garantie ou testée afin de déterminer si elle remplit les exigences qui sont imposées à "un moyen sûr pour la réalisation d'une signature électronique" »[1]. Afin de passer outre cet obstacle, le législateur a décidé « d'assimiler à une signature manuscrite toute signature électronique générée au moyen de la clé de signature de la carte d'identité électronique »[2]. Toutefois, une autre explication à cette dérogation peut être trouvée dans le fait que l'article de loi privilégie un système déterminé pour apposer sa signature, à savoir l'utilisation de la carte d'identité électronique. En optant pour ce procédé spécifique, le législateur fait une entorse au principe de neutralité technologique[3].

3.2.2. Utilisation de l'e-PV en tant que preuve

Au niveau du droit de la preuve, le paragraphe 2 de l'article 100/3 du Code pénal social assimile le procès-verbal signé électroniquement au procès-verbal papier signé à la main. Concrètement, cela signifie qu'en cas de procès, la signature électronique apposée sur l'e-PV sera réputée valable, au même titre qu'une signature manuscrite. Il appartiendra à la partie adverse d'apporter la preuve du contraire. Le législateur ajoute, dans les travaux parlementaires, que « l'e-PV signé de manière électronique par les inspecteurs sociaux est entièrement, notamment en ce qui concerne sa validité et sa valeur probante, assimilé à un procès-verbal établi sur papier et revêtu d'une signature manuscrite »[4]. Cette signature électronique bénéficie de la présomption d'assimilation à une signature manuscrite, car elle remplit les fonctions d'identification, de manifestation du consentement et de maintien de l'intégrité du procès-verbal. Les précisions contenues dans cette disposition légale contribuent à renforcer la sécurité juridique qui entoure le système e-PV.

Par ailleurs, le procès-verbal de constatation d'infractions est revêtu d'une force probante particulière. Par dérogation à la règle du Code d'instruction criminelle proclamant la liberté d'appréciation de la preuve, l'article 66 du Code pénal social dispose

1. Projet de loi-programme, *Doc. parl.*, Chambre, 2011-2012, n° 2081/001, p. 64.
2. Rapport de la Cour des comptes sur la carte d'identité électronique transmis à la Chambre des représentants, Bruxelles, novembre 2012, p. 47.
3. Sur cette notion, voy., notamment, M. Demoulin, *Droit du commerce électronique et équivalents fonctionnels*, Bruxelles, Larcier, 2014, pp. 331 et s.
4. Projet de loi-programme, *Doc. parl.*, Chambre, 2011-2012, n° 2081/001, p. 64.

que les procès-verbaux dressés par les inspecteurs sociaux font foi jusqu'à preuve du contraire, pour autant qu'une copie en soit transmise à l'auteur présumé de l'infraction et, le cas échéant, à son employeur, dans un délai de quatorze jours prenant cours le lendemain du jour de la constatation de l'infraction.

En d'autres mots, seul le procès-verbal constatant des infractions porté à la connaissance du contrevenant dans le délai prescrit est revêtu de cette force probante particulière[1]. Les constatations figurant dans un procès-verbal peuvent être utilisées, avec leur force probante, par les inspecteurs sociaux du même service, des autres services d'inspection ou par les fonctionnaires chargés de la surveillance du respect d'une autre législation[2].

Cela a pour conséquence que le juge doit considérer comme étant véridique le contenu du procès-verbal aussi longtemps que la partie adverse n'a pas démontré l'inexactitude des données qui y sont contenues. Néanmoins, seul l'e-PV est revêtu de cette force probante particulière. L'audition ou le rapport d'enquête ordinaire porté à la connaissance de l'auditeur du travail ou du juge d'instruction ne valent que comme renseignements[3]. Lorsque le contenu d'un procès-verbal n'est pas clair, le juge peut citer l'inspecteur social à comparaître à l'audience pour qu'il fournisse des explications complémentaires relatives à son enquête[4].

Par contre, si le délai légal de notification du procès-verbal n'a pas été respecté, le procès-verbal perd sa force probante particulière[5]. C'est pourquoi le système e-PV prévoit la possibilité pour l'inspecteur social de joindre la preuve de l'envoi recommandé du procès-verbal. En effet, cela permet à l'auditorat du travail et à la DAA de contrôler que le procès-verbal a bien été transmis au contrevenant dans le délai prévu par la loi et donc de s'assurer qu'il est revêtu d'une force probante particulière.

En cas d'égarement de la version papier du procès-verbal signé, qui constitue pour l'instant l'exemplaire original[6], l'e-PV devra être imprimé et signé à nouveau par l'inspecteur. Une copie conforme sera alors éditée par le service d'inspection concerné. Toutefois, il n'est, pour l'instant, pas possible de savoir si un procès-verbal a été imprimé à plusieurs reprises. Dès lors, l'e-PV pourrait être imprimé de multiples fois et étiqueté comme étant la version originale, car rien ne permet de le distinguer de sa copie conforme, mise à part la présence d'une telle mention écrite de la main de l'inspecteur effectuant la copie.

1. *Manuel e-PV, op.cit.*, p.57.
2. Article 67, alinéa 2, C. pén. soc.
3. *Manuel e-PV, op.cit.*, p. 57.
4. *Manuel e-PV, Ibid.*, p. 57.
5. M. Morsa, *op.cit.*, Larcier, 2010, p. 167.
6. Les e-PV constatant exclusivement des infractions de niveau 1 sont considérés, dans leur format électronique, comme étant les originaux.

Enfin, le paragraphe 3 de l'article 100 prévoit la possibilité pour le Roi de perpétuer l'usage du procès-verbal en version papier, selon les modalités et pour la durée qu'Il détermine.

Cette faculté a été mise en œuvre à diverses reprises par le biais d'arrêtés royaux[1] prolongeant la période transitoire au cours de laquelle l'e-PV sera mis sur support papier et signé au moyen d'une signature manuscrite. La fin de la période transitoire était initialement fixée au 31 décembre 2013 par l'arrêté royal du 10 juillet 2013[2]. Cette échéance a ensuite été reportée au 31 décembre 2014 par l'arrêté royal du 26 décembre 2013[3], puis au 31 décembre 2015 par l'arrêté royal du 19 décembre 2014[4].

Cette situation s'explique notamment par le fait que le ministère public n'est pas encore informatisé et n'est donc pas à même de recevoir les procès-verbaux de manière électronique. À deux reprises, il a fallu constater que la transmission électronique des procès-verbaux aux auditeurs du travail à partir des 1er janvier 2014 et 2015 ne s'avérait pas possible.

La distinction entre l'original et la copie du procès-verbal est donc provisoirement maintenue durant la période transitoire. Le procès-verbal imprimé, portant les signatures manuscrites, transmis par la poste à l'auditorat du travail, est encore à considérer comme l'original durant la période transitoire. Le procès-verbal électronique signé et encodé dans la banque de données e-PV doit actuellement être considéré comme étant une copie conforme[5].

Précisons toutefois que les procès-verbaux constatant exclusivement des infractions de niveau 1, c'est-à-dire des infractions uniquement passibles d'amendes administratives, sont transférés seulement à la DAA, et ce, sous format électronique. Dans ce cas, le flux du procès-verbal étant totalement électronique, l'e-PV est considéré comme étant la version originale du document.

Mis à part ce cas spécifique, dans la phase actuelle d'implémentation de l'e-PV, il faut donc encore travailler avec un procès-verbal en version papier, étant donné que les services de la Justice ne sont pas en mesure de participer à l'échange de données électroniques.

---

1. Voy. les articles 2 de l'arrêté royal du 10 juillet 2013, de l'arrêté royal du 26 décembre 2013 et de l'arrêté royal du 19 décembre 2014.
2. Arrêté royal du 10 juillet 2013 portant exécution du chapitre 5 « Réglementation de certains aspects de l'échange électronique d'information entre les acteurs de la lutte contre le travail illégal et la fraude sociale » du titre 5 du livre 1er du Code pénal social, *M.B.*, 31 juillet 2013, p. 47897.
3. Arrêté royal du 26 décembre 2013 modifiant l'arrêté royal du 10 juillet 2013 portant exécution du chapitre 5 « Réglementation de certains aspects de l'échange électronique d'information entre les acteurs de la lutte contre le travail illégal et la fraude sociale » du titre 5 du livre 1er du Code pénal social, *M.B.*, 31 décembre 2013, p. 104070.
4. Arrêté royal du 19 décembre 2014 modifiant l'arrêté royal du 10 juillet 2013 portant exécution du chapitre 5 « Réglementation de certains aspects de l'échange électronique d'information entre les acteurs de la lutte contre le travail illégal et la fraude sociale » du titre 5 du livre 1er du Code pénal social, M.B., 31 décembre 2014, p. 107100.
5. Manuel e-PV, *op. cit.*, p. 59.

À terme, la communication de l'e-PV au ministère public sera prévue et réglée par arrêté royal. En effet, après la phase transitoire au cours de laquelle la communication a lieu au moyen d'un envoi postal, la communication sera réalisée par voie électronique. Dès ce moment, le procès-verbal de constatation d'infractions signé électroniquement vaudra comme document original pour les infractions de tous les niveaux.

4. Conclusion

Au terme de notre analyse du procès-verbal de constatation d'infractions en droit pénal social, il apparaît que des documents subsistent dans leur version papier alors qu'ils pourraient, légalement, exister uniquement sous format numérique. En effet, les inspecteurs sociaux continuent d'envoyer l'original papier à l'auditorat du travail ou au procureur du Roi ainsi qu'une copie au contrevenant. Par ailleurs, les services de police transmettent occasionnellement des procès-verbaux papier aux services d'inspection sociale.

Dans un futur relativement proche, les auditeurs du travail devrait être en mesure de prendre connaissance des e-PV sans qu'il soit nécessaire de les leur envoyer en format papier. Cela permettra un gain de temps, mais aussi un gain financier considérable.

En outre, le développement de l'eBox citoyen[1], sorte de boîte postale électronique officielle, permettra à chaque citoyen de recevoir ses documents officiels émanant des autorités publiques de manière centralisée et sécurisée. Grâce à cet outil, la copie de l'e-PV pourra être envoyée au contrevenant sous forme électronique et permettra de limiter l'envoi de documents papier.

Lors du lancement du projet e-PV, le secrétaire d'État à la Coordination de la lutte contre la fraude voyait l'e-PV comme « un bel exemple de collaboration entre les grands services d'inspection sociale »[2]. De surcroît, il est indéniable que le système e-PV constitue également une belle avancée en termes d'e-gouvernement. Le projet ne s'arrête pas à la rédaction d'un procès-verbal sous forme électronique, mais va plus loin, en prônant la création de flux de données électroniques entre les administrations et en ayant la volonté d'impliquer tous les services d'inspection sociale. Une concertation est actuellement en cours avec les services de police afin de déterminer comment leurs procès-verbaux pourraient être rendus compatibles avec le système

1. À ce sujet, voy. www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/services/basicservices/ebox.html.
2. www.peoplesphere.be/fr/art/3033/un-pv-electronique-pour-tous-les-services-dinspection-sociale.

e-PV. À terme, la Justice devrait également prendre part au projet afin que les e-PV puissent être transmis aux auditeurs du travail de manière électronique et automatisée.

Si la période transitoire n'est pas prolongée une énième fois, le système e-PV devrait être réellement et totalement opérationnel en janvier 2016. La mise en œuvre effective du procès-verbal électronique est indispensable afin de pouvoir parvenir à une consultation des données et à la réalisation de flux électroniques de données entre les différentes administrations et institutions. Ce n'est qu'une fois cet échange de données réalisable que les divers avantages du projet e-PV se matérialiseront.

De ce système e-PV résulteront non seulement une simplification administrative considérable, un fonctionnement plus efficace des services concernés, un traitement accéléré des dossiers, mais aussi et surtout une amélioration de la lutte contre la fraude sociale[1].

1. Projet de loi-programme, *Doc. parl.*, Sénat, 2011-2012, n° 1545/5, p. 5.